economie
FOD Economie, K.M.O., Middenstand en Energie

Europese verordening Nr. 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten

Korte voorstelling

De Europese wetgever nam in 1999 een richtlijn aan tot vaststelling van het juridisch regime dat toepasselijk is op elektronische handtekeningen en op de activiteiten van certificatiedienstverleners[1]. Deze richtlijn werd omgezet in Belgisch recht door de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridische kader voor elektronische handtekeningen en certificatiediensten[2].

Na 15 jaar toepassing vond dezelfde Europese wetgever dat de richtlijn niet voldeed, onder meer door de vaststelling dat de Europese Unie (hierna EU) nog steeds niet over een volledig transnationaal en intersectoraal kader beschikt dat een veilig, betrouwbaar en vlot elektronisch verkeer kan waarborgen dat zowel elektronische identificatie en authenticatie als vertrouwensdiensten andere dan de elektronische handtekening omvat.

Als gevolg van deze vaststelling nam de Europese wetgever de verordening nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/[3] aan.

De hoofddoelstelling van deze verordening is de invoering van een juridisch kader om het vertrouwen in de elektronische transacties in de interne markt te vergroten. Deze verordening trekt de richtlijn van 1999 weliswaar in maar neemt niettemin het merendeel van haar bepalingen over. Hiertoe worden enkele wijzigingen aangebracht en worden een aantal nieuwe bepalingen toegevoegd. Deze bepalingen hebben enerzijds betrekking op de wederzijdse erkenning op EU-niveau van de aangemelde stelsels voor elektronische identificatie en anderzijds op de aanvullende vertrouwensdiensten van de elektronische handtekening (zegel, tijdstempel en de dienst voor elektronische aangetekende verzending alsook de authenticatie van de website).

1. Algemene beschouwingen

1.1. De beoogde doelstellingen van de verordening

Onder de vele beoogde doelstellingen van de verordening kunnen drie belangrijke en verbindende doelstellingen naar voren worden gebracht.

De eerste bestaat erin de belemmeringen, onder meer van juridische en technische aard, voor de werking van de interne markt weg te nemen. Het opheffen van deze verschillende belemmeringen dank zij de verordening moet het in de toekomst onder meer mogelijk maken om zich sneller en gemakkelijker te kwijten van grensoverschrijdende administratieve formaliteiten zoals

- de inschrijving van een student via elektronische weg in een universiteit in het buitenland,
- het online indienen door de belastingbetaler van zijn belastingaangifte in een andere lidstaat,

[1] Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, *PBEG.*, L 13/12 tot 20 van 19 januari 2000.

[2] *B.S*, 29 september 2001, blzn. 33070-33078.

[3] *PBEU* van 28.08.2014, L 257/73 tot 114.

- het vervullen van gezondheidsformaliteiten door een patiënt in het buitenland en zelfs
- het online raadplegen van een medisch dossier door een arts in het buitenland om zo in voorkomend geval te vermijden dat de patiënt die hij verzorgt opnieuw al verrichte onderzoeken en analyses moet ondergaan.

De **tweede** doelstelling beoogt het vertrouwen in de elektronische transacties, vooral dan in de transnationale, te vergroten. Deze doelstelling blijkt zo belangrijk te zijn dat ze vermeld wordt in de titel zelf van de verordening alsook in de eerste regels van de motivering van het voorstel van de Commissie: "In deze toelichting wordt een voorstel voor een wetgevingskader uiteengezet dat bedoeld is om het vertrouwen in elektronische transacties in de interne markt te bevorderen. Het opbouwen van vertrouwen in een online-omgeving is essentieel voor economische ontwikkeling. Een gebrek aan vertrouwen leidt ertoe dat consumenten, bedrijven en overheidsdiensten zullen aarzelen om transacties elektronisch uit te voeren en nieuwe diensten te gebruiken".

Er dient aan herinnerd te worden dat het vertrouwen in de menselijke relaties geen automatische verworvenheid of voldongen feit inhoudt! Net zoals in fysieke menselijke relaties moet vertrouwen ook in de virtuele wereld worden opgebouwd. Het volstaat inderdaad niet om een persoonlijke website te raadplegen of nog om een e-mail of een bericht op een sociaal netwerk te ontvangen van een zogenaamd persoon om automatisch met relatieve zekerheid aan te nemen dat die persoon ook bestaat en wel degelijk de persoon is die hij beweert te zijn en het vertrouwen waard is dat hij beweert te verdienen. Ter overtuiging volstaat het om een kijkje te nemen in onze elektronische mailbox en vast te stellen hoeveel phisingmails er nog elke dag toekomen waarbij identiteitsdiefstal schering en inslag is op het internet. Met de aanneming van de verordening, heeft de Europese Unie uiteindelijk de voorwaarden gecreëerd om dit vertrouwen te waarborgen. Zo reikt ze concrete middelen aan die de burgers, ondernemingen en administraties de mogelijkheid bieden om dit vertrouwen op te bouwen en het onder elkaar uit te testen tijdens hun internetverkeer.

De **derde** doelstelling bestaat erin de rechtszekerheid te versterken zowel ten gunste van de dienstverleners als van de gebruikers van die diensten. Tot nu toe wordt inderdaad vastgesteld dat de markt van de elektronische identificatiediensten evenals van de vertrouwensdiensten ertoe strekt zich verder uit te breiden maar dat verloopt moeilijk en niet altijd even kwaliteitsvol. Hierdoor ontstaan problemen op het vlak van de rechtszekerheid.

De verordening wil een oplossing bieden voor dit probleem. Voortaan zijn de regels die toepasselijk zijn binnen de Europese Unie dezelfde voor iedereen en rechtstreeks toepasselijk in het nationale recht. De lidstaten zijn verplicht om de aangemelde elektronische identificatiemiddelen conform de verordening te erkennen. Zij zijn ook verplicht om de gekwalificeerde vertrouwensdiensten te aanvaarden en de rechtsgevolgen ervan, bekrachtigd door de verordening, te erkennen. De verordening biedt ook aan de verleners van vertrouwensdiensten rechtszekerheid onder meer door hen een relatieve voorspelbaarheid te waarborgen wat vaak een essentiële voorwaarde is bij de beslissing van een marktdeelnemer om te investeren.

Voorts wordt benadrukt dat de verordening niets zegt over de gevallen waarin een identificatie, een handtekening, een datering of een aangetekende verzending juridisch vereist zouden zijn, een zaak die het prerogatief is van de lidstaten. Als dergelijke vereiste echter gesteld wordt door het nationale recht geeft de verordening aan hoe concreet aan deze vereiste kan worden voldaan wanneer de activiteiten in een elektronische omgeving worden verricht.

Achter deze drie doelstellingen gaat de wil verscholen om innovatie en ontwikkeling van het aanbod van vertrouwensdiensten en elektronische identificatiediensten te stimuleren. De positieve effecten van een wetgevend initiatief in termen van het creëren van nieuwe economische diensten en de commerciële ontwikkeling ervan, mogen dus niet worden onderschat.

1.2. De keuze van de verordening als juridisch instrument

Als juridisch instrument opteerde de Europese wetgever voor de verordening, waarvan de bepalingen rechtstreeks toepasselijk zijn in het nationale recht, en niet voor een richtlijn. Juridisch gezien, maakt ze een verdere harmonisatie mogelijk en vermijdt ze verschillen zowel met de juridische interpretatie als de manier om het toezicht uit te oefenen. Vanuit operationeel oogpunt dwingt ze de lidstaten en dienstverleners om doeltreffender samen te werken om de huidige problemen op het gebied van technische interoperabiliteit op te lossen en er zo over te waken dat de nationale systemen – die soms verschillen van elkaar – "elkaar kunnen begrijpen en met elkaar kunnen communiceren".

Een fundamenteel gevolg van de keuze voor de verordening is dat voor de uitvoering ervan uitvoeringshandelingen vereist kunnen zijn. Deze uitvoeringshandelingen worden uiteraard aangenomen op Europees niveau en niet op nationaal niveau. In het onderhavige geval voorziet de verordening in de aanneming van tal van uitvoeringshandelingen (verplichte of optionele) om haar uitvoering te verzekeren (onder meer voor de vertrouwenslijsten, de toezichthoudende instanties, de instellingen voor de conformiteitsbeoordeling, enz.).

1.3. De twee grote luiken van de verordening: de elektronische identificatie en de vertrouwensdiensten

De verordening omvat weliswaar zes hoofdstukken maar het lijdt geen twijfel dat het tweede hoofdstuk over de "elektronische identificatie" en het derde hoofdstuk over de "vertrouwensdiensten"» de meest in het oog springend zijn omdat ze zoveel belangrijke nieuwigheden op die beide gebieden bevatten. De andere vier hoofdstukken (die respectievelijk betrekking hebben op de algemene bepalingen, de gedelegeerde handelingen, de uitvoeringshandelingen en de slotbepalingen) bevatten "bijkomende" bepalingen, hoofdzakelijk ten dienste van de twee voornoemde belangrijke hoofdstukken.

Deze beide hoofdstukken vertonen gemeenschappelijke punten die onder meer met de volgende elementen kunnen worden geïllustreerd.

Ten eerste, de elektronische identificatie die het voorwerp is van het tweede hoofdstuk, vormt een van de aspecten van de elektronische handtekening die op haar beurt behandeld wordt in het derde hoofdstuk. Een belangrijke functie van de handtekening is immers gebaseerd op de identificatie van de ondertekenaar: een document (elektronisch) ondertekenen betekent onder meer zich (elektronisch) identificeren als auteur van dat document.

Een tweede overeenkomst is dat de twee hoofdstukken van de verordening steunen op een evenwicht tussen de vrijwillige systemen enerzijds en de bindende gevolgen anderzijds.

Het tweede hoofdstuk dat de wederzijdse erkenning op EU-niveau van de aangemelde elektronische identificatiemiddelen bekrachtigt, voorziet immers in geen enkele verplichting voor de lidstaten noch om op nationaal niveau een elektronisch identificatiemiddel in te voeren of te gebruiken noch om aan de Commissie een dergelijk middel aan te melden met het oog op grensoverschrijdend gebruik. Wanneer echter een lidstaat (vrij) beslist om onder de voorwaarden van de verordening één elektronisch identificatiemiddel (of meer) aan te melden, voorziet de verordening enerzijds in een verplichting voor alle andere lidstaten om dit aangemelde elektronische identificatiemiddel te aanvaarden en anderzijds in een verplichting

voor de aanmeldende lidstaat om online een authenticatiemiddel te verstrekken om verificatie van de elektronische identificatiegegevens mogelijk te maken.

Op dezelfde wijze voorziet het derde hoofdstuk met betrekking tot de vertrouwensdiensten in geen enkele verplichting voor de lidstaten of voor de dienstverleners om vertrouwensdiensten, al dan niet gekwalificeerde, te verlenen en indien deze voorhanden zijn, ze ook te gebruiken. Wanneer echter een dienstverlener (vrij) beslist om één of meer vertrouwensdiensten te verlenen, moet hij voldoen aan de voorwaarden van de verordening om dergelijke diensten te mogen aanbieden (tenzij ze exclusief gebruikt worden in gesloten systemen voor gebruikers) vooral als ze gekwalificeerd zijn. Bovendien moet een gebruiker van deze diensten kunnen genieten van de rechtsgevolgen erkend door de verordening aan elke van de gekwalificeerde en niet gekwalificeerde vertrouwensdiensten. De nationale rechtscolleges zijn verplicht om deze rechtsgevolgen toe te passen.

Een **derde overeenkomst** tussen de twee hoofdstukken heeft betrekking op de wil om een hoog niveau van betrouwbaarheid te bevorderen, noodzakelijk voor de concretisering van de doelstelling om het vertrouwen te vergroten. De verplichting tot wederzijdse erkenning van de aangemelde elektronische identificatiemiddelen heeft inderdaad enkel betrekking op diegenen die een "substantieel" of "hoog" maar geen "laag" betrouwbaarheidsniveau aanbieden, net zoals een assimilatieclausule of vermoedens van naleving van waarborgen voordeel brengen aan de "gekwalificeerde" vertrouwensdiensten maar niet aan de "gewone of niet-gekwalificeerde" vertrouwensdiensten.

Deze twee hoofdstukken onderscheiden zich van elkaar door volgende elementen.

Vooreerst is hoofdstuk twee hoofdzakelijk beperkt tot de vaststelling van de voorwaarden voor wederzijdse erkenning en interoperabiliteit van de aangemelde identificatiemiddelen met het oog op grensoverschrijdend gebruik ervan. Hoofdstuk drie echter gaat veel verder in de harmonisatie van de regels omdat deze regels niet alleen toepasselijk zijn op het grensoverschrijdende gebruik van de vertrouwensdiensten maar ook op het nationale gebruik ervan.

Daarnaast is het zo, al zijn de grenzen tussen de openbare sector en de privésector niet helemaal waterdicht, dat hoofdstuk twee hoofdzakelijk gefocust is op het gebruik van de elektronische identificatiemiddelen om toegang te krijgen tot een door een openbare instantie aangeboden onlinedienst in de lidstaten. Dit hoofdstuk ligt dus in de lijn van het perspectief om de invoering van het "elektronische bestuur" te vergemakkelijken. Dit hoofdstuk is in de eerste plaats bedoeld voor de publieke actoren. Het derde hoofdstuk echter kan worden vergeleken met een toolkit die zowel ter beschikking wordt gesteld van de openbare besturen voor het uitbreiden van hun applicaties voor elektronisch bestuur als van de actoren uit de privésectoren voor de ontwikkeling van de elektronische handel "Business to Business", "Business to Consumer" en zelfs "Consumer to Consumer". Dit hoofdstuk is zowel voor de openbare actoren als voor de privéactoren bedoeld.

Een laatste fundamenteel verschil tussen beide hoofdstukken ligt in het controlemechanisme. Het hoofdstuk met betrekking tot de elektronische identificatie voorziet in geen enkel controlemechanisme. Afgezien van het feit dat de betrouwbaarheidsniveaus "substantieel" en "hoog" de voorkeur genieten, rekent de verordening op het feit dat de lidstaten niet het risico zouden moeten nemen om één of ander onbetrouwbaar elektronisch identificatiemiddel aan te melden, of dit op lichtzinnige wijze te doen want die aanmelding gebeurt onder hun directe of indirecte aansprakelijkheid en dergelijk middel mag slechts worden aangemeld voor zover het al in de aanmeldende lidstaat werd gebruikt voor de toegang tot minstens één openbare dienst. Hoofdstuk drie echter voert een grondig controlemechanisme in voor de

verleners van vertrouwensdiensten, vooral wanneer de aangeboden diensten gekwalificeerd zijn. In dat geval wordt de controle *a priori* maar ook *a posteriori* uitgevoerd.

2. Het luik betreffende de elektronische identificatie

Een van de doelstellingen van de verordening is om de belemmeringen weg te werken voor het grensoverschrijdend gebruik van de elektronische identificatiemiddelen ter authenticatie, ten minste voor de openbare diensten. Nu deze doelstelling is gesteld, bekijken we nu de maatregelen waarin de verordening voorziet om ze te realiseren.

2.1. De verplichting van wederzijdse erkenning en de verplichting om een authenticatiemiddel te verstrekken

Zoals eerder vermeld, voorziet de verordening in geen enkele verplichting voor de lidstaten noch om op nationaal niveau een elektronisch identificatiemiddel in te voeren of te gebruiken noch om aan de Commissie mee te delen of een of meer van deze middelen op nationaal niveau worden gebruikt met het oog op transnationaal gebruik. De aanmelding op Europees niveau van een elektronisch identificatiemiddel dat op nationaal niveau gebruikt wordt, is dus vrijwillig.

Wanneer een lidstaat beslist om (vrijwillig) onder de voorwaarden van de verordening een elektronisch identificatiemiddel aan te melden, ontstaat voor beide partijen een verplichting: zowel voor de andere lidstaten als voor de aanmeldende lidstaat.

Voor de andere lidstaten legt de verordening hen, mits naleving van een aantal voorwaarden, een verplichting tot wederzijdse erkenning op. Concreet zijn de andere lidstaten verplicht identificatie toe te laten van de onlinediensten die door hun instellingen van de openbare sector verstrekt worden en dit via het door de aanmeldende lidstaat aangemelde identificatiemiddel.

De aanmeldende lidstaat is verplicht om online een authenticatiemiddel te verstrekken om elke vertrouwende partij die gevestigd is op het grondgebied van een andere lidstaat de mogelijkheid te bieden om de elektronische persoonlijke identificatiegegevens te verifiëren en te bevestigen. Deze verplichting bestaat op zijn minst wanneer de vertrouwende partij die gevestigd is op het grondgebied van de andere lidstaat een instantie uit de openbare sector is die haar onlinedienst aanbiedt en die dankzij dit onlineauthenticatiemiddel zo de identiteit van de buitenlandse burger die toegang tot deze dienst wenst, kan verifiëren. De verordening bepaalt dat deze "grensoverschrijdende authenticatie kosteloos is wanneer zij wordt uitgevoerd voor een onlinedienst verleend door een openbare instantie".

Om deze respectieve verplichtingen (verplichting voor de andere lidstaten tot erkenning van de aangemelde elektronische identificatiemiddelen en verplichting voor de aanmeldende lidstaat om een authenticatiemiddel te verstrekken) goed te begrijpen moet een fictief voorbeeld worden gegeven. De Franse staat biedt een openbare dienst aan die zowel aan een Franse burger als aan een andere burger van de Europese Unie de mogelijkheid biedt om over te gaan tot een onlineaanvraag tot inschrijving van een voertuig. Voor toegang tot deze dienst, eist de Franse staat het "substantiële" garantieniveau. Wanneer een Belgische burger toegang wil tot deze Franse dienst via zijn Belgische elektronische identiteitskaart om een Franse inschrijvingsaanvraag in te dienen moet voorafgaand worden nagegaan of de Belgische staat deze kaart bij de Commissie heeft aangemeld en of dit elektronische identificatiemiddel op de lijst staat die in het Publicatieblad is gepubliceerd. Indien dat het geval is en gezien het feit dat de Belgische identiteitskaart overeenstemt met het "hoge" garantieniveau

(te weten, een garantieniveau dat hoger is dan het "substantiële niveau"), heeft de Franse staat de verplichting om de Belgische elektronische identiteitskaart te erkennen en zo de Belgische burger in staat te stellen zich bij zijn aanvraag tot inschrijving met zijn kaart te identificeren. De Belgische staat is verplicht om aan de Franse staat kosteloos een online authenticatiemiddel ter beschikking te stellen om hem als "vertrouwende partij" in staat te stellen de identiteit die de Belgische burger beweert te hebben, te controleren en te valideren via zijn elektronische identiteitskaart.

Tot slot moet er op gewezen worden dat de verplichting tot wederzijdse erkenning enkel betrekking heeft op de doelstelling tot grensoverschrijdende *authenticatie* van een onlinedienst. Met andere woorden, elke lidstaat blijft vrij om de toegangsvoorwaarden tot de dienst, de inhoud van de dienst, het garantieniveau om zich te authenticeren, de manier waarop de dienst wordt verleend, te bepalen en te beslissen of deze dienst al dan niet beschikbaar is voor de aanvrager in overeenstemming met de vooraf vastgestelde categorieën ...

2.2. De voorwaarden van de aanmelding

We hebben weliswaar gezien dat een lidstaat er niet toe gehouden is om een of meer stelsels voor elektronische identificatie die hij eventueel op nationaal niveau gebruikt, aan te melden. Als hij echter beslist om dat te doen, zal hij zich moeten "legitimeren" en voldoen aan tal van voorwaarden als bepaald door artikel 7 van de verordening. Deze voorwaarden streven de hoofddoelstelling van de verordening na, meer bepaald het versterken van het vertrouwen en het optrekken van het veiligheidsniveau.

2.3. De gevolgen van de aanmelding: verplichting in geval van inbreuk op de veiligheid en de aansprakelijkheid

Zodra een stelsel voor elektronische identificatie door een lidstaat wordt aangemeld, vloeien uit de verordening, naast de toepassing van het principe van wederzijdse erkenning, gevolgen voort die zowel betrekking hebben op de inbreuken op de veiligheid als op de aansprakelijkheid.

De verordening bepaalt immers dat wanneer inbreuk wordt gepleegd op het aangemelde stelsel voor elektronische identificatie of op het authenticatiemiddel of wanneer de integriteit ervan deels wordt geschonden "zodat de betrouwbaarheid van de grensoverschrijdende authenticatie van dat stelsel in gevaar komt" de aanmeldende lidstaat onverwijld de grensoverschrijdende authenticatie of de delen waarvan de integriteit geschonden is, moet opschorten of intrekken, en de andere lidstaten en de Commissie hiervan op de hoogte moet brengen.

De verordening handelt over de aansprakelijkheid verbonden aan de aangemelde stelsels voor elektronische identificatie. De aangenomen tekst verdeelt de aansprakelijkheden tussen de verschillende actoren (aanmeldende lidstaat, partij die het elektronische identificatiemiddel *verstrekt* en de partij die de authenticatieprocedure *beheert)* in overeenstemming met hun respectieve interventies.

Er wordt op gewezen dat deze respectieve aansprakelijkheden, bekrachtigd door de verordening, enkel gelden voor de schade veroorzaakt in het kader *van een transnationale transactie.* Voor de nationale transacties is de verordening niet van toepassing en de lidstaten kunnen voorzien in een ander stelsel van gedeelde aansprakelijkheid (uitgebreider of minder uitgebreid).

De verordening bepaalt bovendien dat deze regeling voor aansprakelijkheidsverdeling "niets afdoet aan de aansprakelijkheid uit hoofde van nationale wetgeving van partijen bij een transactie waarin elektronische identificatiemiddelen worden gebruikt die onder het aangemelde

stelsel voor elektronische identificatie vallen". Anders gezegd: de aansprakelijkheidsregeling heeft enkel betrekking op de voornoemde aspecten van het stelsel voor elektronische identificatie maar raakt niet aan de eventuele aansprakelijkheid verbonden aan de inhoud of aan de uitvoering van de transactie zelf tussen de partijen.

3. Het luik over de (gekwalificeerde) vertrouwensdiensten

De hoofddoelstelling van hoofdstuk drie van de verordening, dat gewijd is aan de vertrouwensdiensten, bestaat erin om een algemeen wetgevingskader voor het gebruik van deze diensten in te voeren. In tegenstelling tot de richtlijn 1999/93/EG die zich beperkte tot het reglementeren van de elektronische handtekening en de certificatiedienstverleners dekt de verordening andere vertrouwensdiensten en de dienstverleners die deze diensten aanbieden, zoals het zegel, het tijdstempel en de elektronische aangetekende verzending alsook de authenticatie van een website.

3.1. Algemene principes en gemeenschappelijke basis voor vertrouwensdiensten

3.1.1. De invoering van een optioneel regime en de afwijking voor "gesloten systemen"

Het derde hoofdstuk, over de vertrouwensdiensten houdt geen enkele verplichting in voor de lidstaten of voor de dienstverleners om al dan niet gekwalificeerde vertrouwensdiensten aan te bieden. Wanneer een dienstverlener een of meer vertrouwensdiensten aanbiedt, voorziet de verordening in geen enkele verplichting voor deze dienstverlener om alle door de verordening beoogde vertrouwensdiensten aan te bieden. De verordening verplicht burgers, bedrijven of overheden ook niet om de vertrouwensdiensten die eventueel op de markt worden aangeboden, te gebruiken.

Voorts voorziet de verordening in een afwijking voor "gesloten systemen". De verordening bepaalt inderdaad uitdrukkelijk: " de verordening is niet van toepassing op de verlening van vertrouwensdiensten die uitsluitend gebruikt worden in systemen die gesloten zijn als gevolg van nationaal recht of overeenkomsten tussen een welbepaalde groep deelnemers".

3.1.2. Gekwalificeerde versus niet-gekwalificeerde vertrouwensdiensten

De verordening berust weliswaar op een optioneel systeem maar toch moet eraan herinnerd worden dat wanneer een dienstverlener (vrij) beslist om een of meer vertrouwensdiensten aan te bieden, hij moet voldoen aan de voorwaarden van de verordening om dergelijke diensten te kunnen aanbieden, zeker wanneer het gekwalificeerde diensten betreft. Bovendien moet een gebruiker van deze diensten kunnen genieten van de rechtsgevolgen die de verordening aan elk van de gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten toekent en de nationale rechtscolleges moeten deze rechtsgevolgen erkennen.

De verordening maakt een groot onderscheid tussen *gekwalificeerde* en *niet-gekwalificeerde* vertrouwensdiensten. De gekwalificeerde vertrouwensdiensten en de dienstverleners die ze aanbieden, zijn onderworpen aan tal van strikte voorwaarden wat niet het geval is voor de niet-gekwalificeerde diensten.

In die context zou men zich terecht kunnen afvragen welk belang men er zou kunnen bij hebben om eerder gebruik te maken van een gekwalificeerde dienst dan van een niet-gekwalificeerde dienst. Dit belang kan worden aangetoond aan de hand van twee belangrijke elementen.

In de eerste plaats zal de keuze afhangen van de juridische strategie en van het beleid betreffende risicobeheer van de gebruiker waarbij wordt aangestipt dat niet *a* priori een voorbarig oordeel kan worden geveld over de (gebrekkige) kwaliteit van een niet-gekwalificeerde vertrouwensdienst. Wanneer iemand deze diensten gebruikt op een gebied waar een laag veiligheids- en betrouwbaarheidsniveau volstaan en/of voor juridische handelingen waarbij het risico op betwistingen gering en zelfs aanvaardbaar is, kan die persoon zich tevredenstellen met een niet-gekwalificeerde dienst. Wanneer een gebruiker echter gebruik maakt van deze diensten op een gebied waar een hoog veiligheidsniveau vereist is omdat er grote risico's op aanvallen of fraude bestaan en/of voor juridische handelingen waarvoor men geen risico op betwisting kan riskeren omdat de (financiële of andere) inzet te groot is, zal hij de raad krijgen om gebruik te maken van een gekwalificeerde vertrouwensdienst.

Een tweede reden waarom de voorkeur gegeven wordt aan een van beide types dienst, vindt zijn oorsprong in de rechtsgevolgen die eraan verbonden zijn en de juridische voorzienbaarheid die eruit voortvloeit.

Alle gekwalificeerde vertrouwensdiensten genieten inderdaad van een gelijkstellingsclausule of van veronderstellingen, waardoor de gebruiker ervan wordt vrijgesteld van de bewijslast in geval van betwisting. Zo bepaalt artikel 25.2. dat "Een gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening", artikel 35.2. dat "Voor een gekwalificeerd elektronisch zegel het vermoeden geldt van integriteit van de gegevens en van juistheid van de oorsprong van de gegevens waaraan het gekwalificeerde elektronisch zegel is verbonden", artikel 41.2. dat "voor een gekwalificeerd elektronisch tijdstempel het vermoeden geldt van de juistheid van de aangegeven datum en het aangegeven tijdstip, en van de integriteit van de gegevens waaraan de datum en het tijdstip zijn gekoppeld", artikel 43.2. dat "voor gegevens die via een gekwalificeerde dienst voor elektronisch aangetekende bezorging worden verstuurd en ontvangen, het vermoeden geldt van integriteit van de gegevens, van de verzending van die gegevens door de geïdentificeerde afzender, van de ontvangst daarvan door de geïdentificeerde geadresseerde, en van de nauwkeurigheid van de datum en het tijdstip van verzending en van ontvangst, zoals aangegeven door de gekwalificeerde dienst voor elektronisch aangetekende bezorging".

De niet-gekwalificeerde vertrouwensdiensten echter genieten "enkel" van de niet-discriminatieclausule waarbij geacht wordt dat het rechtsgevolg en de ontvankelijkheid van de niet-gekwalificeerde vertrouwensdienst als bewijs voor het gerecht niet mogen worden geweigerd alleen omdat deze dienst in elektronische vorm wordt aangeboden of omdat hij niet voldoet aan de vereisten van dezelfde gekwalificeerde vertrouwensdienst. In geval van betwisting is het dus aan de gebruiker van deze diensten om te bewijzen dat zij voldoende betrouwbaar zijn en om de rechter te overtuigen van het feit dat zij de waarborgen bieden die normaal van deze diensten worden verwacht.

3.1.3. Procedure van voorafgaande vergunning voor het initiëren van een gekwalificeerde vertrouwensdienst en vertrouwenslijst

De gekwalificeerde vertrouwensdiensten en de verleners die ze aanbieden, zijn onderworpen aan veel striktere vereisten dan die welke gelden voor niet-gekwalificeerde diensten wat onder meer de bevoorrechte rechtsgevolgen (gelijkstellingsclausule en veronderstellingen) die eraan worden toegekend, rechtvaardigt. Een van deze vereisten is de voorafgaande vergunning. Deze procedure moet absoluut gevolgd en afgerond worden voordat gekwalificeerde vertrouwensdiensten worden aangeboden in tegenstelling tot niet-gekwalificeerde vertrouwensdiensten die aan geen enkele vergunning, voorafgaande procedure of formaliteit zijn onderworpen.

Concreet: wanneer een dienstverlener het voornemen heeft om een gekwalificeerde vertrouwensdienst (of meer) te gaan aanbieden, moet hij bij het toezichthoudende orgaan een kennisgeving van zijn voornemen indienen, evenals een door een conformiteitsbeoordelingsorgaan afgegeven conformiteitsbeoordelingsverslag.

Het toezichthoudende orgaan verifieert of de verlener van vertrouwensdiensten en de door hem verleende vertrouwensdiensten in overeenstemming zijn met de eisen vastgelegd in de verordening. Als dat het geval is, kent het aan de verlener van vertrouwensdiensten en aan de door hem verleende vertrouwensdienst de "status van gekwalificeerde" toe en stelt het orgaan dat verantwoordelijk is voor het opstellen en onderhouden van de "vertrouwenslijsten" hiervan in kennis, ten laatste drie maanden na de oorspronkelijke kennisgeving van de dienstverlener.

Gekwalificeerde verleners van vertrouwensdiensten mogen niet beginnen met het verlenen van de gekwalificeerde vertrouwensdienst zolang de status van "gekwalificeerde" niet in de vertrouwenslijst is opgenomen.

De vertrouwenslijsten zijn een van de hoekstenen van de verordening. Zij zijn immers veilig en op elk moment online toegankelijk waardoor elke gebruiker gemakkelijk en op betrouwbare manier kan controleren of de verlener waarop hij een beroep wil doen, wel degelijk is opgenomen in de lijst en over de "status van gekwalificeerde" beschikt.

3.1.4. Het EU-vertrouwensmerk voor de gekwalificeerde vertrouwensdiensten

Men zal moeten erkennen dat vertrouwen in en gebruiksgemak van onlinediensten voor gebruikers van wezenlijk belang zijn om maximaal te kunnen profiteren van en bewust te vertrouwen op elektronische diensten. Daartoe voorziet de verordening in de invoering van een EU-vertrouwensmerk ter aanduiding van de door gekwalificeerde verleners van vertrouwensdiensten verleende gekwalificeerde vertrouwensdiensten. Op die manier zou dit label gekwalificeerde vertrouwensdiensten duidelijk onderscheiden van andere vertrouwensdiensten, wat tot markttransparantie zou bijdragen.

Het gebruik van dit label door de gekwalificeerde dienstverleners moet vrijwillig zijn. Desgevallend moet de dienstverlener er voor zorgen dat er op zijn website voorzien is in een link naar de betrokken vertrouwenslijst.

3.1.5. Toezichtregeling

In navolging van de verordening 1999/93/EG, legt de verordening de lidstaten op om een doeltreffende regeling in te voeren om toezicht te houden op de verleners van vertrouwensdiensten. De verordening gaat echter nog veel verder door de bekrachtiging van een verplichting voor de lidstaten om een toezichthoudend orgaan aan te wijzen en door de bevoegdheid van dit orgaan te preciseren en uit te breiden. Deze ontwikkeling geeft de wil weer van de Commissie en van de Europese wetgever om de toezichtregeling niet alleen te versterken maar ook uitgebreider te harmoniseren. Deze regeling werd tot nog toe als te "kwetsbaar" aanzien in het kader van de richtlijn, onder meer omwille van de veel te grote vrijheid die aan de lidstaten wordt gelaten.

Het toezichthoudende orgaan moet toezicht houden op alle verleners van al dan niet gekwalificeerde vertrouwensdiensten. De rol van dit orgaan zal gevoelig variëren naargelang van de categorie waartoe de gecontroleerde dienstverlener behoort.

Ofwel betreft het een *gekwalificeerde* verlener van vertrouwensdiensten en in dat geval moet het orgaan toezicht houden op de verleners van vertrouwensdiensten "die gevestigd zijn in de aanwijzende lidstaat om door middel van toezichthoudende activiteiten *vooraf* en *achteraf* te

waarborgen dat deze gekwalificeerde verleners van vertrouwensdiensten en de door hen verleende gekwalificeerde vertrouwensdiensten voldoen aan de eisen in deze verordening". Zij worden dus *vooraf* gecontroleerd in het kader van de procedure voor het opstarten van een gekwalificeerde vertrouwensdienst maar ook *achteraf* in het kader van een periodieke audit (om de twee jaar) van een eventuele buitengewone audit op vraag van het toezichthoudende orgaan of nog als gevolg van een eventuele kennisgeving door de dienstverlener van een inbreuk op de veiligheid. De verordening legt de kosten verbonden aan de voornoemde audit ten laste van de dienstverleners.

Ofwel betreft het een *niet-gekwalificeerde* verlener van vertrouwensdiensten en in dat geval moet het orgaan "enkel *indien nodig* tegen verleners (...) die gevestigd zijn in de aanwijzende lidstaat optreden door middel van toezichthoudende activiteiten *achteraf, wanneer het orgaan verneemt dat* deze niet-gekwalificeerde verleners van vertrouwensdiensten of de door hen verleende vertrouwensdiensten niet zouden voldoen aan de vereisten van deze verordening".

3.1.6. Aansprakelijkheid van de verleners van vertrouwensdiensten

De tekst over de aansprakelijkheid van de verleners van vertrouwensdiensten maakt een duidelijk onderscheid tussen gekwalificeerde en niet-gekwalificeerde dienstverleners.

- Als het een *niet-gekwalificeerde* verlener van vertrouwensdiensten betreft, ligt de bewijslast bij de natuurlijke persoon of de rechtspersoon die de schade heeft ondergaan. Hij moet dus bewijzen dat de dienstverlener, met opzet of door nalatigheid, zijn verplichtingen bedoeld in de verordening niet heeft nageleefd en dat de schade te wijten is aan dit verzuim.
- Als het echter een *gekwalificeerde* verlener van vertrouwensdiensten betreft, ligt de bewijslast bij deze dienstverlener. Hij wordt inderdaad aansprakelijk gehouden tenzij hij aantoont dat de schade die te wijten is aan het verzuim zijn verplichtingen bedoeld in de verordening na te leven, niet met opzet of door nalatigheid uit zijn hoofde werd toegebracht.

Dit onderscheid is hoofdzakelijk gerechtvaardigd door de wil van de Europese wetgever om de niet-gekwalificeerde dienstverleners geen te zware juridische regeling op te leggen en het risico te lopen de ontwikkeling van deze categorie dienstverleners af te remmen, te meer daar de diensten die door de laatstgenoemden worden aangeboden niet genieten van "stimulansen" die voortvloeien uit de bovenvermelde gelijkstellingsclausules of veronderstellingen.

Bovendien biedt de verordening de verleners van vertrouwensdiensten de mogelijkheid om hun aansprakelijkheid contractueel te regelen. De verordening laat hen immers toe om onder twee voorwaarden beperkingen te verbinden aan het gebruik van de door hen verleende diensten. Ten eerste moeten de klanten vooraf terdege worden geïnformeerd over de beperkingen. Ten tweede moeten deze beperkingen herkenbaar zijn voor een derde partij, bijvoorbeeld doordat er informatie over de beperkingen wordt opgenomen in de voorwaarden met betrekking tot de verleende dienst, of via andere herkenbare middelen. In voorkomend geval worden ze niet aansprakelijk gehouden voor de schade die te wijten is aan het gebruik van diensten en die deze beperkingen te buiten gaat.

3.1.7. Internationale aspecten

In een gemondialiseerde economie en een internetomgeving waar geen grenzen bestaan, kon in de verordening geen bepaling ontbreken om de "gunstige gevolgen" van de verordening buiten de Europese Unie uit te breiden.

Zo bepaalt de verordening dat "vertrouwensdiensten verstrekt door in een derde land gevestigde verleners van vertrouwensdiensten rechtens erkend worden als gelijkwaardig aan gekwalificeerde vertrouwensdiensten verstrekt door gekwalificeerde, in de Unie gevestigde verleners van vertrouwensdiensten, indien de vertrouwensdiensten die afkomstig zijn uit het derde land, worden erkend op grond van een overeenkomst, gesloten tussen de Unie en het betrokken derde land of een internationale organisatie". Voortaan kunnen gekwalificeerde vertrouwensdiensten enkel op grond van de internationale overeenkomst buiten de grenzen van de Unie erkend worden.

De Europese wetgever heeft er ook voor gezorgd dat de dienstverleners gevestigd in de Unie genieten van het wederkerigheidsprincipe. Zo geldt dat "de door in de Unie gevestigde, gekwalificeerde verleners van vertrouwensdiensten geleverde gekwalificeerde vertrouwensdiensten worden erkend als wettelijk gelijkwaardig aan vertrouwensdiensten van verleners van vertrouwensdiensten in het derde land of de internationale organisatie waarmee de overeenkomst is gesloten".

3.2. Elektronische handtekeningen

Afdeling 4 van hoofdstuk 3 over de elektronische handtekeningen is wellicht de afdeling die het minste aantal nieuwigheden in de verordening biedt, in die zin dat ze voor een groot stuk de bepalingen van richtlijn 1999/93/EG overneemt, weliswaar na een aantal herformuleringen, preciseringen, schrappingen en toevoegingen.

Wat de rechtsgevolgen van de elektronische handtekeningen betreft, omvat de verordening de al bekende clausules over niet-discriminatie enerzijds en over gelijkstelling anderzijds die bekrachtigd werden in de richtlijn. Ze vereenvoudigt echter de formulering van deze clausules waardoor ze gemakkelijker te lezen en te begrijpen zijn.

De verordening bepaalt dat een *gekwalificeerde* elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. De verordening gaat niet verder in de harmonisatie. Daarom moet het nationale recht bepalen welk het rechtsgevolg is van de handgeschreven handtekening.

Het rechtsgevolg van een *niet-gekwalificeerde* handtekening mag niet worden ontkend (louter) op grond van het feit dat de handtekening elektronisch is of niet aan de eisen voor gekwalificeerde elektronische handtekeningen voldoet. Voor het overige moet ook hier het nationale recht bepalen welke de rechtsgevolgen van niet-gekwalificeerde elektronische handtekeningen zijn.

Artikel 28 bepaalt de eisen die toepasselijk zijn op gekwalificeerde certificaten voor elektronische handtekeningen waarbij dit artikel zelf verwijst naar de technische eisen in bijlage I. We onthouden dat deze lijst met eisen maximaal is. Om grensoverschrijdende interoperabiliteit en erkenning van de gekwalificeerde certificaten te verzekeren, kunnen de lidstaten inderdaad niet voorzien in andere dwingende eisen.

De verordening maakt het op nationaal niveau echter mogelijk om specifieke kenmerken in gekwalificeerde certificaten te doen opnemen, mits die specifieke kenmerken niet verplicht zijn en de grensoverschrijdende interoperabiliteit en erkenning van gekwalificeerde elektronische handtekeningen niet hinderen.

De verordening brengt vernieuwing ten aanzien van de richtlijn, in die zin dat ze vereisten over het proces en de dienst betreffende *validering* van de gekwalificeerde elektronische handtekeningen vaststelt. Deze bepalingen moeten ervoor zorgen dat valideringsdiensten overal worden toegepast waardoor de vertrouwende partijen het resultaat van de beoorde-

ling van een gekwalificeerde elektronische handtekening op een geautomatiseerde, betrouwbare en efficiënte manier kunnen ontvangen.

Tot slot wordt opgemerkt dat de verordening het gebruik van pseudoniemen in elektronische transacties toelaat en meer bepaald in certificaten voor elektronische handtekeningen. In voorkomend geval moet duidelijk worden aangegeven dat het een pseudoniem betreft.

3.3. Elektronische zegel versus elektronische handtekening

Deze nieuwe vertrouwensdienst die gecreëerd werd door de verordening waarborgt de link tussen de "verzegelde" elektronische gegevens en een rechtspersoon. Het betreft een soort van beveiligde elektronische "stempel" voor rechtspersonen. De verordening bepaalt "elektronische zegels moeten dienen als bewijs dat een elektronisch document door een rechtspersoon is afgegeven, door zekerheid over de oorsprong en integriteit van het document te garanderen". Ze voegt er nog aan toe "behalve voor de authenticatie van het door de rechtspersoon afgegeven document, kunnen elektronische zegels worden gebruikt voor de authenticatie van alle digitale activa van de rechtspersoon, zoals softwarecode of servers".

De technologie alsook de hardware en software die gebruikt worden om een elektronisch zegel aan te maken, zijn weliswaar identiek met die welke gebruikt worden om een elektronische handtekening aan te maken, maar toch onderscheidt het elektronische zegel zich fundamenteel van de elektronische handtekening, in die zin dat de elektronische handtekening voorbehouden is voor natuurlijke personen en het zegel bestemd is voor rechtspersonen. Een tweede fundamenteel verschil ligt in de gevolgen die respectievelijk aan de elektronische handtekening en aan het elektronische zegel verbonden zijn: de elektronische handtekening wordt *gebruikt om te ondertekenen* en zo de ondertekenende natuurlijke persoon te verbinden terwijl het zegel de rechtspersoon in de zin van de verordening niet kan verbinden maar beperkt blijft tot *het garanderen van zekerheid omtrent de oorsprong en integriteit van de "verzegelde" elektronische gegevens".*

Over de rechtsgevolgen van de elektronische zegels bevat de verordening ook twee clausules.

- De eerste bepaalt: "Het rechtsgevolg van een elektronisch zegel en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures mogen niet worden ontkend louter op grond van het feit dat het zegel elektronisch is of niet aan de eisen voor gekwalificeerde elektronische zegels voldoet".
- De tweede clausule omvat een weerlegbaar vermoeden volgens hetwelke: "Voor een gekwalificeerd elektronisch zegel geldt het vermoeden van integriteit van de gegevens en van juistheid van de oorsprong van de gegevens waaraan het gekwalificeerde elektronische zegel is verbonden".

3.4. Elektronische tijdstempel

De "elektronische tijdstempel" (in het Engels "time stamping") wordt in de verordening gedefinieerd als "gegevens in elektronische vorm die andere gegevens in elektronische vorm verbinden aan een bepaald tijdstip en die bewijzen dat die laatstgenoemde gegevens op dat tijdstip bestonden". Het gebruik van een dienst om te "dateren" kan vaak al dan niet om juridische redenen nuttig zijn. Hij kan dienen om elektronische documenten zoals contracten, eenzijdige verbintenissen, opzeggingen, ontslagbrieven, geding inleidende stukken, enz. te "dateren". Maar er kunnen ook evenementen zoals de toegang tot een document, het verzenden van een document, het sluiten van een transactie of het afsluiten van een dossier mee worden "gedateerd".

Gezien het belang van dit type dienst in het kader van de elektronische transacties vond de Europese wetgever het nuttig om er net zoals voor de andere vertrouwensdiensten een plaats aan te geven.

Over de rechtsgevolgen van de elektronische tijdstempel omvat de verordening opnieuw twee clausules.

- De eerste bepaalt: "Het rechtsgevolg van een elektronisch tijdstempel en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures mogen niet worden ontkend louter op grond van het feit dat het stempel elektronisch is of niet aan de eisen voor gekwalificeerde elektronische tijdstempels voldoet".
- De tweede clausule omvat een weerlegbaar vermoeden ten gunste van de gekwalificeerde elektronische tijdstempels: "Voor een gekwalificeerd elektronisch tijdstempel geldt het vermoeden van de juistheid van de aangegeven datum en het aangegeven tijdstip, en van de integriteit van de gegevens waaraan de datum en het tijdstip zijn gekoppeld".

3.5. Dienst voor elektronische aangetekende verzending (bezorging)

De verordening definieert de dienst voor elektronische aangetekende verzending als "een dienst die het mogelijk maakt gegevens via elektronische middelen tussen derden te verzenden en die bewijs verschaft ten aanzien van het hanteren van de verzonden gegevens, met inbegrip van bewijs van het verzenden en ontvangen van de gegevens, en die de verzonden gegevens beschermt tegen het risico van verlies, diefstal, beschadiging of onbevoegde wijzigingen". Het betreft *grosso modo* een elektronisch equivalent van de fysieke of papieren elektronische verzending die we al tientallen jaren kennen in het postwezen, d.w.z. een elektronische dienst die een relatieve zekerheid (technisch en juridisch) kan bieden over het feit dat elektronische gegevens verzonden en ontvangen werden op integere manier en ook over de datum van verzending en ontvangst van deze gegevens.

Deze dienst wordt in vele lidstaten weliswaar nog niet op algemene wijze gebruikt maar de Europese wetgever ziet er een gelegenheid in om nieuwe mogelijkheden te bieden om hem te commercialiseren.

Wat de rechtsgevolgen van de elektronische aangetekende verzending betreft, omvat de verordening ook twee clausules.

- De eerste bepaalt: "Het rechtsgevolg en toelaatbaarheid als bewijsmiddel in gerechtelijke procedures van gegevens die via een dienst voor elektronisch aangetekende bezorging verstuurd en ontvangen worden, mogen niet worden ontkend louter op grond van het feit dat de dienst elektronisch is of niet aan de eisen voor de gekwalificeerde dienst voor elektronisch aangetekende bezorging voldoet".
- De tweede clausule omvat een weerlegbaar vermoeden ten gunste van de gekwalificeerde aangetekende elektronische bezorging: "Voor gegevens die via een gekwalificeerde dienst voor elektronisch aangetekende bezorging worden verstuurd en ontvangen, geldt het vermoeden van integriteit van de gegevens, van de verzending van die gegevens door de geïdentificeerde afzender, van de ontvangst daarvan door de geïdentificeerde geadresseerde, en van de nauwkeurigheid van de datum en het tijdstip van verzending en van ontvangst, zoals aangegeven door de gekwalificeerde dienst voor elektronisch aangetekende bezorging".

In tegenstelling tot de fysieke aangetekende verzending die doorgaans aan de verzender de mogelijkheid biedt om al dan niet een ontvangstbewijs te vragen, heeft de Europese wetgever

het ontvangstbewijs blijkbaar uitgebreid voor de elektronische aangetekende verzending en deze functionaliteit beschouwd als een wezenlijk bestanddeel van de dienst. Met andere woorden, wanneer een dienst voor elektronische aangetekende verzending aangeboden of gebruikt wordt, heeft de verzender niet langer de mogelijkheid om te kiezen voor de aangetekende verzending zonder ontvangstbewijs.

3.6. Authenticatie van websites

Het hoofddoel van de dienst authenticatie van de website bestaat erin de authenticiteit van de link tussen een website en de verantwoordelijke ervan te garanderen. Ontelbaar zijn vandaag het aantal handelsnamen die slachtoffer werden van "phishing", d.w.z. van oplichters die valse websites maken, conforme kopieën van de echte website, om zich uit te geven als een firma of een natuurlijke persoon (bv. in de banksector of in de verhuur van vakantiewoningen) om de wat naïeve internetgebruikers geldbedragen af te troggelen. Met als doelstelling het vertrouwensklimaat te versterken in het kader van online commerciële transacties, beoogt deze dienst voor authenticatie van de website om de internetgebruikers, met een gekwalificeerd certificaat voor website-authenticatie, de echtheid en de legitimiteit van de website te garanderen en het feit dat de natuurlijke persoon of de rechtspersoon aangeduid als verantwoordelijke van de site wel degelijk de persoon is die hij beweert te zijn.

Het verlenen door de dienstverlener en het gebruik door de verantwoordelijken van de websites van deze authenticatiedienst van websites gebeuren volledig op vrijwillige basis en vormen geen belemmering voor het gebruik of het aanbod van andere middelen of methodes die authenticatie van een website mogelijk maken.

3.7. Elektronische documenten

De verordening omvat een niet-discriminatieclausule ten aanzien van elektronische documenten: "Het rechtsgevolg van een elektronisch document en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures mogen niet worden ontkend louter op grond van het feit dat het document elektronisch is". Deze bepaling is weliswaar minimalistisch maar in elk geval tracht ze het gebruik van elektronische documenten aan te moedigen en iedere discriminatie ten opzichte van papieren documenten te vermijden.

4. Slotbepalingen: inwerkingtreding, toepassing en overgangsmaatregelen

In het laatste hoofdstuk over de slotbepalingen vinden we de elementen die inzicht geven in de progressieve uitvoering van de verordening vanaf de publicatie ervan in het Publicatieblad van de Europese Unie op 28 augustus 2014. Zo bevat dit hoofdstuk bepalingen over de inwerkingtreding, de toepassing, de opheffing van de richtlijn 1999/93/EG, de overgangsmaatregelen en de toekomstige herziening van de verordening.

Om de Commissie de kans te bieden om het proces van goedkeuring van de uitvoeringshandelingen onmiddellijk op te starten maar ook om de lidstaten de tijd te laten om zich voor te bereiden en/of hun systemen aan te passen aan de bepalingen van de nieuwe verordening, maakt de verordening een onderscheid tussen de inwerkingtreding van de verordening en de toepassing van de bepalingen ervan.

De verordening is op 17 september 2014 in werking getreden, te weten op de twintigste dag na publicatie in het PBEU. Zodoende moet gewacht worden tot 1 juli 2016 om de fundamentele wijzigingen die aan de verordening werden aangebracht concreet te beschouwen.

Het principe is immers dat de verordening toepasselijk is vanaf 1 juli 2016, met uitzondering echter van een reeks bepalingen bedoeld in de tweede paragraaf van artikel 52, die ofwel voor ofwel na 1 juli 2016 van toepassing worden.

In grote lijnen moet vooral worden onthouden dat de bepalingen over de vertrouwensdiensten van toepassing worden vanaf 1 juli 2016, met uitzondering van de bepalingen over de goedkeuring van de (optionele of verplichte) uitvoeringshandelingen die noodzakelijk zijn voor het aanbod en de goede werking van de vertrouwensdiensten. Het proces van goedkeuring van deze handelingen werd voor alle duidelijkheid door de Commissie opgestart in 17 september 2014 (en zelfs voor die datum in het kader van een informele groep van deskundigen).

Voor de bepalingen over de elektronische identificatie is de situatie complexer. Wat vooral moet onthouden worden, is dat het proces van goedkeuring van de uitvoeringshandelingen vanaf 17 september 2014 van start ging en dat de, vanaf 18 september 2015, vrijwillige erkenning van de aangemelde elektronische identificatiemiddelen op 18 september 2018 ten vroegste verplichtend wordt.

Aangezien de verordening bepaalt dat de richtlijn 1999/93/EG opgeheven wordt met ingang op 1juli 2016, bleek het belangrijk om te voorzien in overgangsmaatregelen om certificatiedienstverleners die conform deze richtlijn werkten rechtszekerheid te bieden. Om deze dienstverleners dus de mogelijkheid te bieden om hun diensten verder te blijven aanbieden met inachtneming van de bepalingen van de verordening, bepaalt artikel 51 enerzijds dat veilige middelen voor het aanmaken van handtekeningen overeenkomstig de richtlijn beschouwd worden als gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen in de zin van de onderhavige verordening en anderzijds worden de gekwalificeerde certificaten voor natuurlijke personen in de zin van de richtlijn, totdat zij verlopen, beschouwd als gekwalificeerde certificaten voor elektronische handtekeningen in de zin van de onderhavige verordening.

Artikel 51 voegt er aan toe dat een certificatiedienstverlener die gekwalificeerde certificaten overeenkomstig Richtlijn 1999/93/EG afgeeft, zo spoedig mogelijk, maar niet later dan 1 juli 2017, een conformiteitsbeoordelingsverslag indient bij het toezichthoudend orgaan. Tot de indiening van dat conformiteitsbeoordelingsverslag en de voltooiing van de beoordeling ervan door het toezichthoudend orgaan wordt die certificatiedienstverlener beschouwd als een gekwalificeerde verlener van vertrouwensdiensten in de zin van deze verordening. De dienstverlener beschikt dus over een termijn van één jaar vanaf de toepassing van de verordening om zijn situatie te regulariseren. Indien deze dienstverlener niet binnen de opgegeven termijn een conformiteitsbeoordelingsverslag indient of indien het toezichthoudende orgaan vindt dat het verslag niet overtuigend is, wordt deze certificatiedienstverlener vanaf 2 juli 2017 niet beschouwd als gekwalificeerde verlener van vertrouwensdiensten in de zin van de verordening. Daarom kunnen wij de dienstverleners die gekwalificeerde certificaten afgeven enkel maar aanraden om de goedkeuring van de uitvoeringshandelingen van nabij te volgen en om zich geleidelijk conform te stellen met de bepalingen van de nieuwe verordening om mogelijke problemen te vermijden vanaf 2 juli 2017.

FOD Economie, K.M.O., Middenstand en Energie
December 2014

Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.